OA a SŠP
Veselí nad Moravou

ITík

BŘEZEN 2025

Číslo 7

KYBERBEZPEČNOST

TIPY A TRIKY

ZE SVĚTA UMĚLÉ INTELIGENCE

Obsah

Úvodní slovo

Milí čtenáři,
březnový ITík je tu a s ním i důležitá témata – **kyberbezpečnost a autorské právo**. Naučíme vás, jak si ověřit, zda vaše hesla neunikla, jak se chránit před phishingem a proč se vyplatí používat správce hesel.
Také se podíváme na **autorský zákon ve škole** – co můžete legálně použít ve výuce a jak správně citovat zdroje. Právě tomuto tématu se budeme věnovat i na 7. IT středě, kam vás srdečně zveme!
Nezapomněli jsme ani na novinky ze světa AI – představíme vám **DigiDay #23**, který se zaměřil na efektivní komunikaci s umělou inteligencí.
Příjemné čtení!

Jindřich Zdráhal

REDAKTOR

Všechny texty a spousta obrázků v ITíku vznikají za větší nebo menší pomoci umělé inteligence – využívám chatGPT od společnosti OpenAI.
Texty neprochází jinou jazykovou korekturou než od AI.

JSTE V BEZPEČÍ?
Uniklo vaše heslo? Jak se chránit?

Kyberbezpečnost už dávno není jen téma pro IT odborníky – týká se nás všech. Každý den se objevují nové phishingové podvody, úniky hesel a škodlivé odkazy. Jak si tedy ověřit, zda jsou vaše účty v bezpečí? A co dělat, pokud zjistíte, že vaše heslo uniklo? V tomto článku se podíváme na nástroje a tipy, které vám pomohou ochránit vaše digitální soukromí.

Uniklo vaše heslo? Zjistěte to během pár vteřin!

Na internetu existuje už několik miliard uniklých hesel. Pokud si říkáte, že vás se to netýká, možná se budete divit. Stačí navštívit stránku Have I Been Pwned, zadat svůj e-mail a zjistit, zda se někdy objevil v některém z úniků dat. Pokud ano, je čas změnit heslo – a ideálně pro každý účet jiné.

Co dělat, když moje heslo uniklo?

1. **Okamžitě ho změňte** – pokud uniklo heslo, které stále používáte, změňte ho co nejdříve.
2. **Nikdy nepoužívejte stejné heslo pro více účtů** – pokud útočníci získají vaše heslo z jedné stránky, mohou ho vyzkoušet jinde.
3. **Zapněte si dvoufázové ověření (2FA)** – pokud to služba umožňuje, přidejte si dodatečnou vrstvu zabezpečení.

Odkaz v e-mailu? Pozor, může to být past!

Phishing je jednou z nejčastějších kybernetických hrozeb. Podvodné e-maily nebo weby se snaží vylákat vaše přihlašovací údaje pod falešnou záminkou. Jak je poznat?

🔴 **Podezřelá adresa odesílatele** – Pokud dostanete e-mail od „banka@secur1ty-check.com", zbystřete. Firmy nikdy neposílají oficiální e-maily z podivných domén.

🔴 **Naléhavý tón** – „Váš účet byl zablokován! Klikněte ihned sem!" Podvodníci spoléhají na paniku, abyste klikli bez přemýšlení.

🔴 **Zkrácené nebo upravené odkazy** – Před kliknutím na odkaz si ho vždy zkontrolujte. Stačí nad něj najet myší a podívat se na skutečnou adresu.

Jak si ověřit, zda je odkaz nebo soubor bezpečný?

📌 Použijte službu VirusTotal, která umí analyzovat odkazy a soubory pomocí desítek antivirů.

Bezpečná hesla: Jak je mít pod kontrolou?

Používání jednoduchého hesla jako „123456" nebo „heslo123" je jako nechávat klíč pod rohožkou. Jak tedy mít bezpečné a přitom zapamatovatelné heslo?

✔ **Používejte dlouhá a složitá hesla** – alespoň 12 znaků, kombinaci písmen, čísel a speciálních znaků.

✔ **Nikdy nepoužívejte stejné heslo dvakrát** – pokud útočník získá jedno, měl by se nedostat k dalším účtům.

✔ **Používejte správce hesel** – aplikace jako Bitwarden nebo peněženka na iPhonu si hesla zapamatují za vás.

📢 **Bonusový tip:** Pokud si nechcete pamatovat složitá hesla, zkuste větu místo hesla – například "MojePrvníKoloJelo50km!" je mnohem bezpečnější než „123456" a přitom zapamatovatelné.

Závěr: Opatrnost se vyplácí!

Kyberhrozby se neustále vyvíjejí, ale s trochou prevence se můžete vyhnout většině z nich. Stačí si pravidelně kontrolovat, zda vaše heslo neuniklo, být obezřetní při otevírání e-mailů a používat silná hesla. A hlavně – pokud něco vypadá podezřele, raději si to dvakrát ověřte, než na to kliknete!

Buďte v bezpečí! 🔐

TIPY A TRIKY

Než kliknete na podezřelý odkaz, můžete si ho rychle ověřit! Stačí na něj najet myší (bez kliknutí) a v levém dolním rohu prohlížeče se zobrazí skutečná adresa. Pokud vypadá podezřele (např. místo banky.cz vidíte banky-secure-login.com), raději na něj neklikejte.

Po pořízení screenshotu pomocí [WIN] + [SHIFT] + [S] ho můžete rovnou otevřít v Malování a pomocí nástroje „Obdélník" nebo „Štětec" začernit osobní údaje.

Používáte stejná hesla na více stránkách? Nechte si je bezpečně spravovat! Nepoužívejte, ale možnost "uložit heslo do prohlížeče" Místo toho zkuste doplněk s nějakým správcem hesel, třeba Bitwarden.

ZE SVĚTA AI:

DigiDay #23

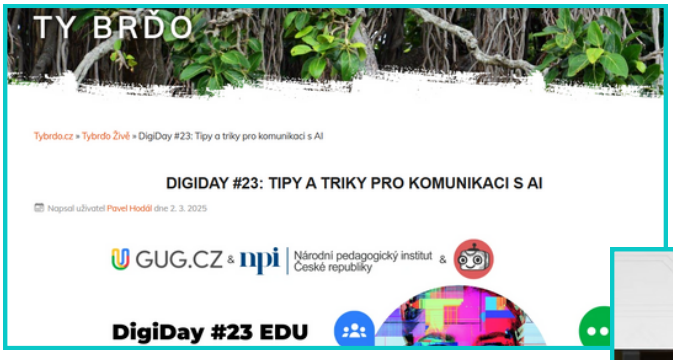
V rámci série DigiDay se 20. ledna 2025 uskutečnil 23. díl s názvem **Komunikace s AI - tipy a triky**. Tento online seminář se zaměřil na efektivní využití umělé inteligence ve vzdělávání a představil pokročilé techniky komunikace s AI, které mohou učitelům usnadnit práci a obohatit výuku.

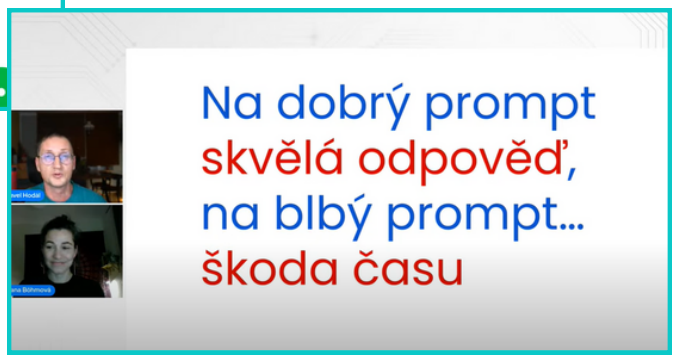
Hlavní témata DigiDay #23

- **Tipy a triky pro komunikaci s AI**: Jak efektivně formulovat dotazy (prompty) pro získání kvalitních odpovědí od AI.
- **Hlasoví asistenti ve výuce i osobní agendě**: Využití hlasových asistentů pro organizaci práce a interakci se studenty.
- **Pokročilé promptování**: Techniky pro tvorbu komplexních a specifických dotazů, které umožní AI poskytovat přesnější a užitečnější informace.
- **Možnosti AI v napojení na API**: Jak propojit AI s dalšími aplikacemi a službami pomocí API pro rozšíření jejích funkcionalit.

Pro zájemce je k dispozici záznam z akce na youtubu.
Hlavní organizátor této akce – Pavel Hodál k tomu sepsal na svém webu "Ty brďo" článek.

Zajímavostí je, že tento článek shrnující DigiDay vznikl za použití nástroje NotebookLM od společnosti Google o kterém jsme se tady již bavili. Tento AI asistent umožňuje uživatelům nahrávat různé dokumenty, jako jsou PDF soubory, YouTube videa či webové články, a následně z nich generovat shrnutí nebo odpovídat na specifické otázky týkající se obsahu.





https://tybrdo.cz/zive/

POZVÁNKA

7. IT STŘEDA

19. 3. 2025
PO VYUČOVÁNÍ
UČEBNA UCE

Víte, co si můžete stáhnout a použít ve výuce? Jak je to s kopírováním materiálů? A co když chcete využít umělou inteligenci k tvorbě obsahu? Autorský zákon ve škole je téma, které se týká nás všech – učitelů, studentů i škol jako institucí.
Na této IT středě si jasně a srozumitelně vysvětlíme:
✅ Co můžete (a nemůžete) používat ve výuce podle autorského zákona.
✅ Jak správně citovat a jaké zdroje lze legálně využít.
✅ Jak se na autorské právo dívají nástroje jako Canva, ChatGPT nebo YouTube.
✅ Kde hledat volně dostupné obrázky, hudbu a texty.
Přijďte si rozšířit obzory a ujasnit pravidla, která jsou důležitá nejen pro školu, ale i pro běžný život v digitálním světě!

O UMĚLÉ INTELIGENCI

3. 4. 2025
17.00 – 19.00
MULTIMEDIÁLNÍ UČEBNA

Zveme vás na povídání o umělé inteligenci, které se uskuteční 3. dubna 2025 v 17:00 v budově OA. Odpovíme si na otázky, co vlastně AI je, jak funguje, kde ji najdeme a jaké přínosy i rizika s sebou přináší. Ukážeme si některá použití i možnosti zneužití.
Přijďte si rozšířit obzory a dozvědět se více o technologii, která mění svět! Vstup je zdarma.

ITík

Školní IT občasník vydávaný na
OA a SŠP Veselí nad Moravou

OA a SŠP
Veselí nad Moravou

ITík | Číslo 07
Březen 2025

jihomoravský kraj
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání